

Reporters How-To's

Here you will find supplementary content for reporters, including step-by-step instructions and examples for relevant topics.

- [Version History](#)
- [How to resend and activation email \(for organization managers only\)](#)
- [How to validate an E5X-file \(for organization managers only\)](#)
- [How to understand user status \(for organization managers only\)](#)

Version History

Version	Date	Document	Description	E2 release
0.1	04/11/2025	How to understand user status.docx	Initial version	2.53
0.1	12/05/2025	How to resend an activation email.docx	Initial version	2.47
0.1	17/06/2024	How to validate an E5X-file.docx	Initial version	2.35
0.2	20/11/2025	How to understand user status	Migration to BookStack platform.	2.53
0.2	20/11/2025	How to resend an activation email	Migration to BookStack platform.	2.47
0.2	20/11/2025	How to validate an E5X-file	Migration to the BookStack platform - section concerning organization reporters.	2.35

How to resend and activation email (for organization managers only)

What is an activation email?

An activation email is sent when a user account is created. It contains a hyperlink to the account activation page. This link is active for 72 hours after having been sent.

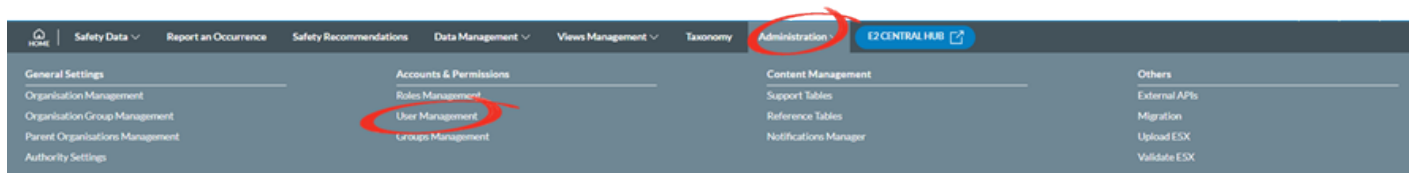
Steps to resend

An activation email cannot be resent as such. However, following these steps will mimic the activation process

Step 1

Access the user account

As an Organisation Manager or as a National Security manager you need to activate the user account



Step 2

Set the disabled switch to off (left)

User Account Details

Account Type: **Individual** Organisation M2M

Authority:* EASA

Organisation:

Username:*

Description:

Creation Date: 06-Jun-2023 08:57:46 Modification Date: 06-Jun-2023 08:57:46

Last Activity:

☒ Disabled ☐ Blocked

▼ PROPERTIES

▼ ROLES

Step 3

Open the E2 logon page and click on forgot password (in an other browser that the one your are currently in)

ECCAIRS2 - SRIS2

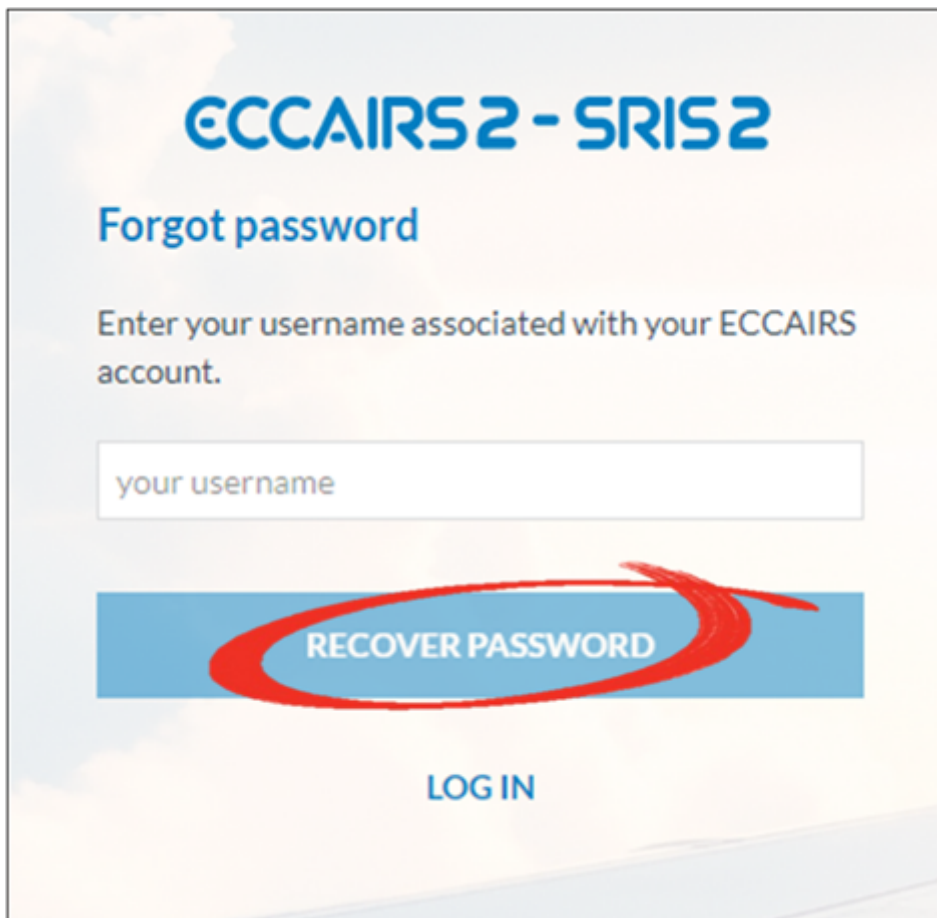
Sign in



Forgot your password

Step 4

Enter the username (not the email address) and click recover password



ECCAIRS2 - SRIS2

Forgot password

Enter your username associated with your ECCAIRS account.

RECOVER PASSWORD

LOG IN

An email will be sent to the email address attached to the username

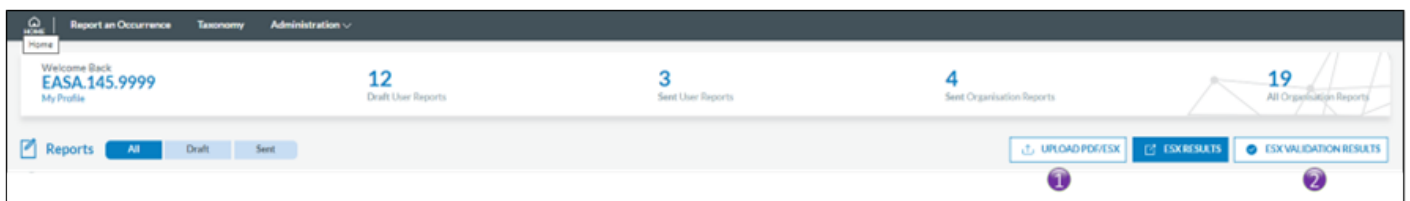
How to validate an E5X-file (for organization managers only)

Who can validate an e5x-file

Only users of registered organisations and Authority users can submit e5x-files. Therefore, it is their prerogative to also validate e5x-files and not submitting them to their Authority

In many cases users of registered organisations and Authority users have an IT service that generates an e5x-file based on data stored in a legacy system. Allowing the IT service to validate, that is check, the e5x-file, E2 caters for e5x-file validation.

As a user from a registered organisation



The validation Interface

From the home page a direct access to the e5x validation is provided by clicking on the Upload PDF/E5X button

1. Upload PDF/E5X

Upload

Format: PDF e5x

Upload the filled form. A maximum of 50 files and 600MB is allowed

Select files... Done

GRH test trial.e5x

CANCEL VALIDATE UPLOAD

1. By selecting e5x, the validation button will appear
2. Click either on select files, or drag and drop the files on top of the “Drop files here”; It is possible to validate >1 e5x-file at the time
3. Click on validate and the validation process will start. You will get an email conformation that the e5x-file(s) was(were) uploaded. The file(s) is(are) put on a processing queue, that means that they are not validated immediately
4. This interface is also used for directly uploading e5x-files, no prior validation will be done and upon success or partial success the e5x-file will be submitted to the Authority

View validation results

2. E5X Validation results

Results

BACK

Username	Filename	Authority	Total Reports N°	Total Attachments	Initial Process Date	Final Process Date	Validation status
	ID714CE23AAA6CA7CBA05F124BCC3598A.zip	EASA	1	0	24-May-2024 11:18:14	24-May-2024 11:18:17	Processed with Errors
	CAB test.zip	EASA	1	0	13-May-2024 10:11:22	13-May-2024 10:11:25	Processed with Errors
	EVL24-013_2024-04-03.zip	EASA	1	4	04-Apr-2024 14:41:07	04-Apr-2024 14:41:59	Processed OK
	EVL24-013_2024-04-03.zip	EASA	1	4	04-Apr-2024 14:38:33	04-Apr-2024 14:39:08	Processed with Errors
	179287.zip	EASA	1	0	11-Jan-2024 16:12:53	11-Jan-2024 16:12:56	Processed with Errors
	1310230221607738eb64ac44e932.zip	EASA	1	1	13-Oct-2023 11:30:08	13-Oct-2023 11:30:10	Processed with Errors
	OC-EASA-2023004101.zip	EASA	1	0	22-Aug-2023 12:49:13	22-Aug-2023 12:49:17	Processed with Errors
	OC-EASA-2023004101.zip	EASA	1	0	22-Aug-2023 12:44:37	22-Aug-2023 12:44:41	Processed with Errors
	OC-EASA-2023005047.zip	EASA	1	0	14-Aug-2023 09:29:20	14-Aug-2023 09:29:23	Processed with Errors
	OC-EASA-202300678.zip	EASA	1	0	14-Aug-2023 09:28:43	14-Aug-2023 09:28:47	Processed OK

1 - 10 of 15 items

1. Navigating with the mouse to the last column, allows for downloading the validation logfile in case the validation was processed with error.
- The Validation logfile is a CSV-file that can be opened in excel or equivalent as can be seen in the example

	A	B	C	D	E	F	G	H	I	J
1	ESz/ESx Id	File Name	User Id	Authority Name	Total Reports	Total Attachments	Initial Process Date	Final Process Date	Validation Status	Message
2	49530	GRH test trial.zip	EASA,145,9999	EASA	1	0	2024-05-27 07:41:01.0	2024-05-27 07:41:04.0	Validated with Errors	
3										
4		XML Id	XML FileName	File Number	Responsible Entity	Initial Process Date	Final Process Date	Validation Status	Message	
5		3785254	ID54CB31A3957A4E32B5F9323EF4C8AA66	null	33	2024-05-27 07:41:02.0	2024-05-27 07:41:02.0	Not validated	Error processing ESz xml: Error extracting entities from xml: The entities with tags: ATTRIBUTES, are not included in current taxonomy mapping	
6										

2. It is possible to limit the number of rows shown by applying filters in the column headers
- Filters are type sensitive that is depending on the type of column a filter is applied, different filter methods are available

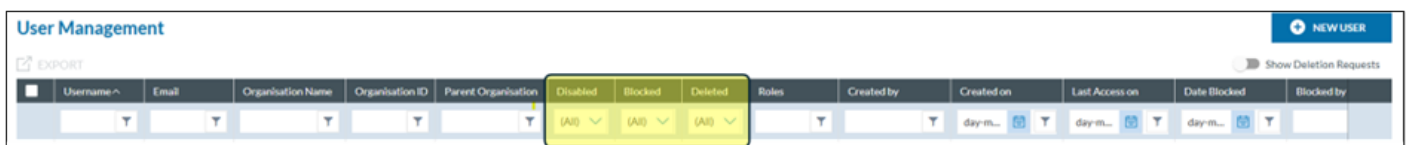
How to understand user status (for organization managers only)

Purpose

Understanding the complexity of different user statuses has long been a challenge. Moreover, a user's status, and the way it is set, can often be interpreted in multiple ways.

This document aims to clarify the various user statuses, explain how they are assigned, and specify who has the authority to set them.

What user status do exist?



The screenshot shows a 'User Management' interface. At the top right is a 'NEW USER' button. Below it is a table with columns: Username, Email, Organisation Name, Organisation ID, Parent Organisation, Disabled, Blocked, Deleted, Roles, Created by, Created on, Last Access on, Date Blocked, and Blocked by. The 'Disabled', 'Blocked', and 'Deleted' columns are highlighted in yellow and each contains a dropdown menu with '(All)' selected. There is also an 'EXPORT' button and a 'Show Deletion Requests' toggle.

Username	Email	Organisation Name	Organisation ID	Parent Organisation	Disabled	Blocked	Deleted	Roles	Created by	Created on	Last Access on	Date Blocked	Blocked by
					(All)	(All)	(All)			day-m...	day-m...	day-m...	

Deleted

- When a user request for his account to be deleted, all fields except his username are anonymised. Consequentially his status will be set to deleted
- When an Authority or an organisation is deleted, then all its users are deleted too.
- An organisation manager or an Authority National Security Administrator cannot delete a user account

Blocked

An account can only be blocked by an administrator. Whether it be an organisation manager or an Authority National Security Administrator. This often happens when users are no longer active in an organisation or in an Authority.

Users trying to login with their blocked account are requested to contact the administrator.

Disabled

An account can only be disabled by the system. It is automatically done when certain conditions are met. Such as inactivity for more than 90 days. An organisation manager or an Authority National Security Administrator, cannot directly change this.

As this status can only be set by the system, the slide button is greyed out.



Who can do which actions?

Unblocking an account

It is the prerogative of organisation manager or an Authority's National Security Administrator that can unblock an account which was previously blocked.

When unblocking an account, the user account will also be automatically enabled by the system

Deleting an organisation

Only a National Security Administrator can delete an organisation, which will set all user accounts to deleted

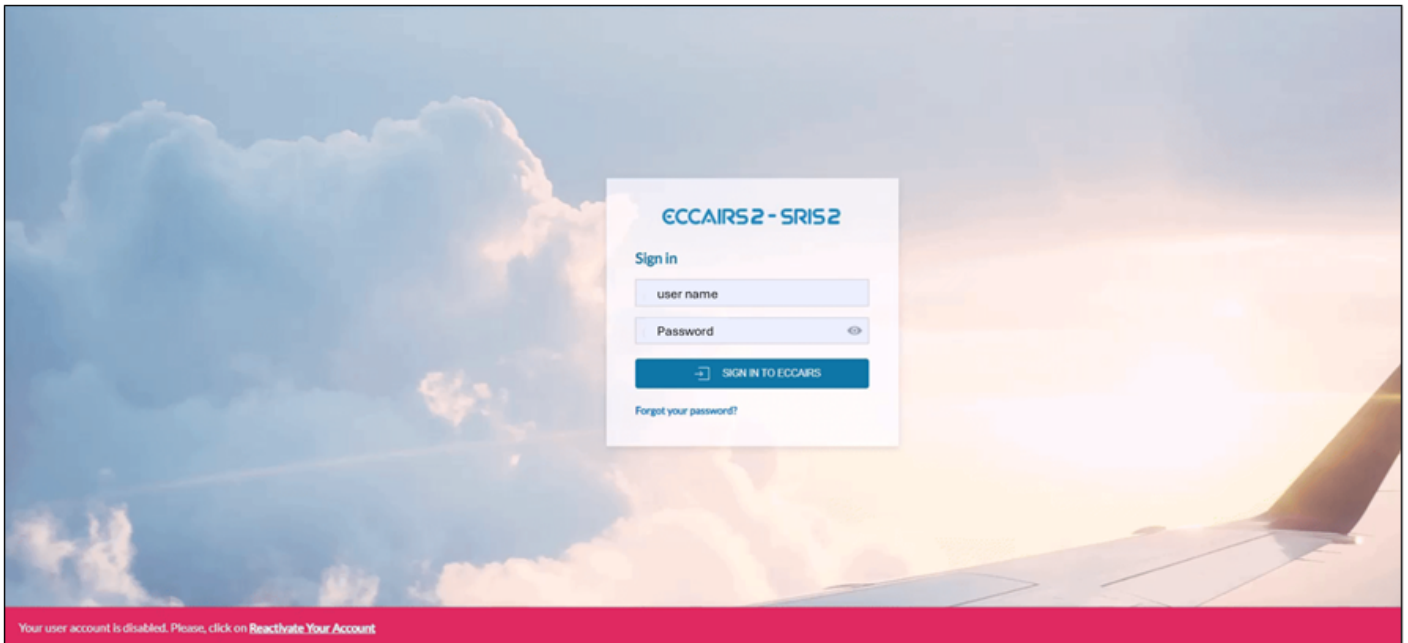
Deleting an Authority

Only an ECCAIRS system administrator may delete an Authority setting all user accounts, organisation and Authority users, to deleted

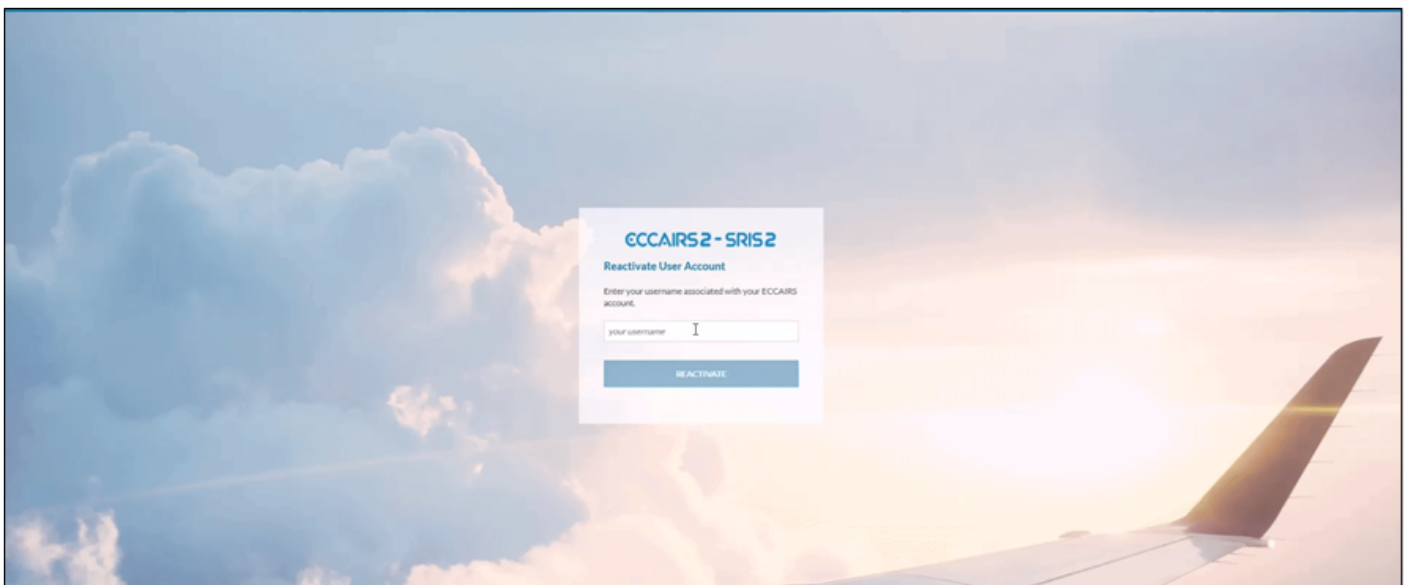
Re-enabling

An account that is disabled by the system and which is not blocked by an organisation manager or an Authority's National Security Administrator can be re-enabled by the user

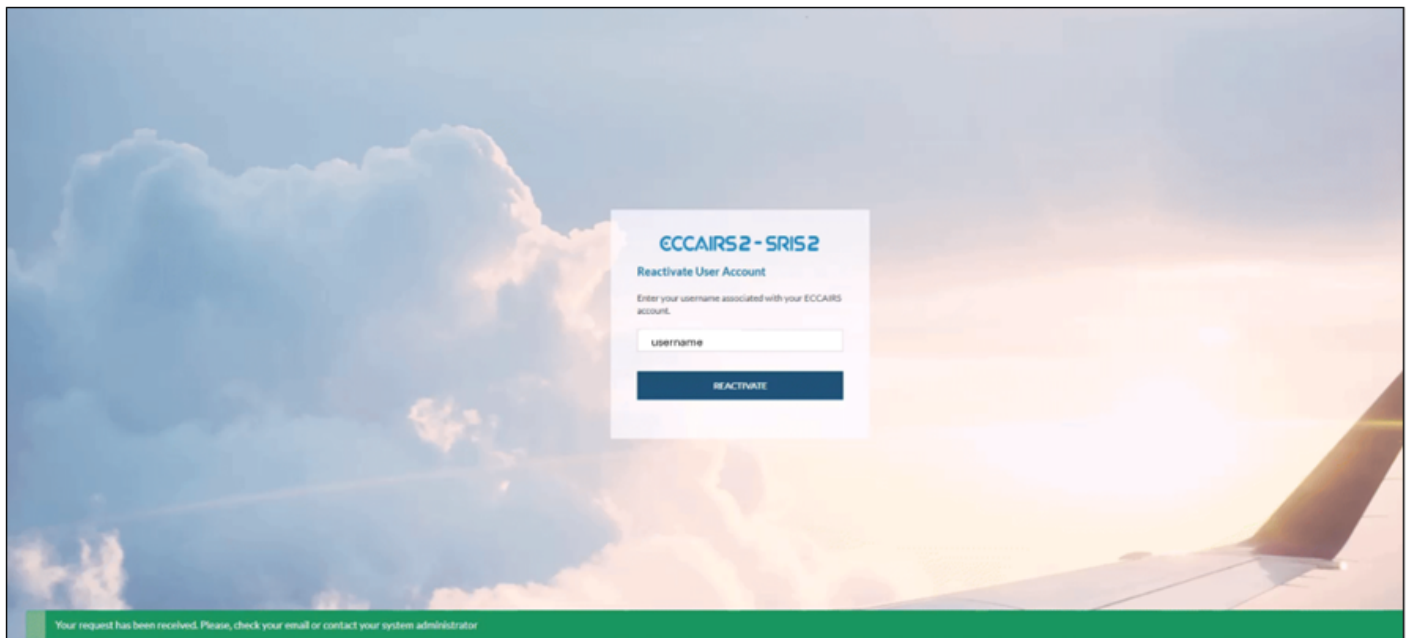
- The user logs in with his correct username and password. If his account is disabled, a red banner with a hyperlink to reactivate his account will be shown at the bottom of the screen



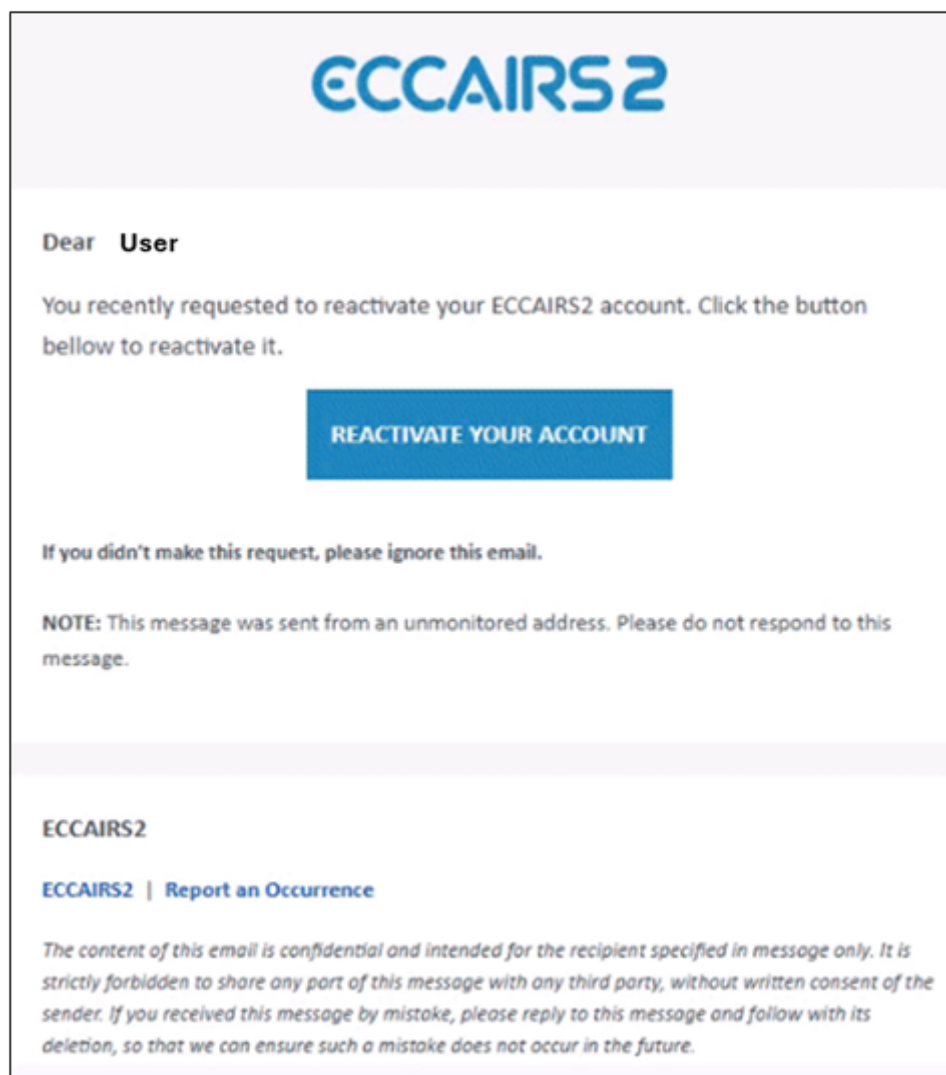
- In the next window, the username is to be entered



An acknowledge banner is shown informing the user that a reactivation email was sent to the email address linked to his account.



To reactivate the account, the user is to click on the “Reactivate your account” button



By confirming the reactivation will finalise the re-activation exercise

